TTB IT Security Rules of Behavior

U.S. Government systems are for authorized use only.
Use of the TTB systems constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities.

NOTE: These IT Security Rules of Behavior are applicable to all individuals with access to TTB information systems

1. Do not access information systems or sensitive data without proper authorization. Use the TTB Electronic 7200 (E-7200) Information Systems Access Process to make requests for any information system access (http://ttbweb/forms/7200-process.html)

2. Never write down your passwords or PIN numbers unless they are stored in a secure place (like a physical safe or in an encrypted file). This is especially critical for the RSA devices. Loss of the RSA device coupled with a written PIN allows direct access to TTB resources.

3. Do not access, browse, research, or change any account, file, data, record, or application not required to perform your official duties. You are prohibited from performing any of the aforementioned actions for personal interest. If you have a legitimate need to conduct official business, and have been granted access to the system, you may access, research, or change the account, file, record, or application only to the extent required to conduct your official business.

4. Protect employee privacy rights. You should consider the effects of your actions on the privacy of individuals. As an example, TTB personnel may have private phone numbers or birth date data on the TTB Intraweb. Taking this data outside of TTB may be a violation of an employee's privacy rights.

5. Protect all Personally Identifiable Information (PII) from disclosure. PII is information that can be used to uniquely identify an individual (such as SSN or name and home address). The loss of such information could lead to many potentially damaging effects on an individual, such as identity theft.

6. The transmission of Personally Identifiable Information (PII), 6103 Tax Data, or any other sensitive data outside of the TTB environment is prohibited unless the data is encrypted.

7. Protect all of your authentication credentials (username and password) from disclosure. You are responsible for any computer activity associated with your username. Do not share your username and password with any other individuals, regardless of their position in or outside of TTB.

8. Authentication credentials must be distributed and reset using a secure process. Do not accept a password unless you feel it was delivered in a secure manner. If given the option, immediately change your password after initial logon to any information system.

9. Do not program your authentication credentials into automatic script routines or programs. If a login prompt asks to save or remember your username and/or password, always responds no.

10. Immediately change any default passwords for any TTB information systems. If you think that a password has been compromised, change your password and immediately notify your supervisor.

11. Do not install or use unauthorized hardware or software. Also do not exchange system components. All hardware and software must be documented, tested, authorized and approved for use by the Office of the Chief Information Officer in accordance with TTB's configuration management plan.

12. Do not use privately owned hardware, software or media to process, access, or store TTB information without written approval of the Chief Information Officer. SSL VPN (use of your home computer to access the TTB network) access is an exception to this and its use is specifically authorized in the TTB remote access policy, including additional rules of behavior specific to that system. Privately owned equipment shall not be connected to TTB systems and the TTB network.

13. Personnel should take every precaution to physically protect portable media, including laptop computers. Some examples of physically protecting portable media include locking it in a safe, keeping it on your person, and securing laptops with laptop cable locks. The requirement to physically secure laptop computers exists everywhere: in your office, while traveling, in temporary lodging and in your home.

14. Protect all TTB computer equipment from hazards such as liquids, food, smoke, etc.

15. Retrieve all hard copy printouts in a timely manner. If you cannot determine the originator or receiver of a printout, dispose of it in a waste container used specifically for sensitive data.

16. Protect any removable storage media (e.g., magnetic, optical, flash/thumb drives, etc.) from exposure to electrical currents, extreme temperatures, bending, fluids, smoke, etc. Ensure that all removable storage media is properly labeled and protected based on the sensitivity of the information contained. You are prohibited from storing sensitive data on removable media (USB hard drive, flash drive, CD, DVD). All sensitive data on removable media must be encrypted.

17. You must take every precaution to avoid storing sensitive, unencrypted data on any removable or portable media, including laptop hard drives. For those employees who are absolutely required to transport and access sensitive data to perform their mission function, the following applies:

    a. The first storage location of choice for sensitive data is the database application (don't extract the data in the first place), second choice is your personal network drive (the G drive).

    b. If you MUST have sensitive data on removable media such as CD's, DVD's or USB thumb drives, the sensitive data *must be encrypted*. Detailed procedures to encrypt the data have been developed. Contact the TTB Help Desk for assistance with the correct means to protect AND RETRIEVE your sensitive data. Again, you should carefully weigh the need to transport sensitive data against the risk involved.

18. Lock or log off from any workstation that you are using when you go to lunch, take a break, or anytime you leave the workstation.

19. Employees are permitted to use government office equipment, including IT resources for personal purposes on a limited basis, when such use involves minimal additional expense to the Government and does not overburden any of TTB's information resources. Please reference *TTB O 7321.1 Personal Use of Government Office Equipment, Including Information Technology Resources*, for additional clarification as needed.

20. Employees are prohibited from using the Internet to access pornography, gambling, hacker sites, or any other site that may be deemed inappropriate. If you have any question on what may be considered inappropriate, ask your supervisor BEFORE accessing the site.

21. Back up critical data and store it in a safe place. These backups should be performed regularly and the data/media should be protected in accordance with the sensitivity of the data contained in the backup.

22. Use TTB provided and properly configured equipment and software (e.g. TTB laptop/VPN or SSL VPN) for remote access TTB information systems and data from home, hotels, customer sites, etc. Please reference *TTB O 7320.1, Remote Access Policy* for additional rules of behavior for remote access to TTB systems.

23. Observe all software licensing agreements. Do not violate Federal Copyright laws. If you have any questions about copyright or licensing, contact the Office of Chief Counsel BEFORE using the material in question.

24. Do not disclose or discuss any TTB-related information with unauthorized individuals. Depending on the nature of the information, unauthorized disclosure would not only constitute a violation of TTB policy and directive and could result in employee discipline but such a willful unauthorized disclosure could violate a number of different criminal statutes, including, for example, the Internal Revenue Code, 26 U.S.C. 6103, and/or The Privacy Act, 5 USC 552a and result in prosecution, fines and jail time.

25. Employees are required to acknowledge these Rules of Behavior before they will be granted access privileges to any TTB information system. Failure to do so will cause access privileges to be disabled.

26. Promptly report all security incidents, no matter how insignificant they may appear, to the TTB Information Security Office (ttb_infosec@ttb.gov; 202-453-0220) or Jackie Washington (Jackie.washington@ttb.gov; 202-453-2019). These security incidents can include unauthorized disclosure of information, computer viruses, theft of equipment or data, deliberate alteration or destruction of data or equipment, etc.

CONDUCT WHICH DOES NOT CONFORM TO THESE RULES MAY FORM THE BASIS FOR APPROPRIATE DISCIPLINARY ACTION. PENALTIES CAN RANGE FROM REPRIMAND FOR A MINOR INFRACTION TO REMOVAL FROM THE FEDERAL SERVICE OR CRIMINAL PROSECUTION FOR THE MOST SERIOUS VIOLATIONS.

TTB IT Security Rules of Behavior

By signing this form, the user acknowledges that he/she has read and will abide by the TTB IT Security Rules of Behavior for information systems.

____________________/_________________________ ____________________________

Print Name / Signature Date